WHAT IS CLAIMED IS:

1. A method for providing automated tracking of security vulnerabilities, comprising:

performing a vulnerability assessment on a system;

storing data obtained from the vulnerability assessment in a vulnerability database;

determining a vulnerability score based on a plurality of vulnerability factors identified by the vulnerability assessment; and

determining a time to fix a vulnerability identified by the vulnerability assessment of the system based on the determined vulnerability score.

2. The method of claim 1, wherein determining the vulnerability factor further comprises considering the frequency the identified vulnerability occurs in the system.

3. The method of claim 2, wherein determining the vulnerability factor further comprises the criticality of an element in the system presenting the vulnerability and a rating of the severity of the vulnerability.

4. The method of claim 1 further comprising determining an IP address associated with the vulnerability.

5. The method of claim 4 further comprising entering the IP address and a description of the identified vulnerability in a tracking database.

6. The method of claim 1 further comprising determining delinquent vulnerabilities based upon the determined time to fix the vulnerability identified by the vulnerability assessment.

7. The method of claim 6 further comprising providing notification of determined delinquencies.

8. The method of claim 6 further comprising re-running a scan profile when notification is received that the vulnerability has been fixed.

9. The method of claim 8 further comprising determining whether the vulnerability still exists and archiving records associated with the vulnerability when the vulnerability does not still exist.

10. A method for determining a criticality factor for a vulnerability in a computer system, comprising:

entering in a database vulnerabilities identified during a vulnerability assessment;

monitoring a frequency of occurrence for the identified vulnerabilities; and

assigning a vulnerability factor to a vulnerability based upon the frequency of occurrence of the vulnerability in the system.

11. The method of claim 10, wherein the assigning a vulnerability factor further comprises considering a criticality of an element in the system presenting the vulnerability and a rating of the severity of the vulnerability within the system.

12. An apparatus for providing automated tracking of security vulnerabilities, comprising:

a memory for storing program instructions; and

a processor, configured according to the program instructions for performing a vulnerability assessment on a system, storing data obtained from the vulnerability assessment in a vulnerability database, determining a vulnerability score based on a plurality of vulnerability factors identified by the vulnerability assessment and determining a time to fix a vulnerability identified by the vulnerability assessment of the system based on the determined vulnerability score.

13. The apparatus of claim 12, wherein the processor considers a frequency of the identified vulnerability in the system when determining the vulnerability factor.

14. The apparatus of claim 13, wherein the processor further considers the criticality of an element in the system presenting the vulnerability and a rating of the severity of the vulnerability when determining the vulnerability factor.

15. The apparatus of claim 12, wherein the processor determines an IP address associated with the vulnerability.

16. The apparatus of claim 15, wherein the processor enters the IP address and a description of the identified vulnerability in a tracking database.

17. The apparatus of claim 12, wherein the processor identifies delinquent vulnerabilities based upon the determined time to fix the vulnerability identified by the vulnerability assessment.

18. The apparatus of claim 17, wherein the processor provides notification of the identified delinquencies.

19. The apparatus of claim 17, wherein the processor re-runs a scan profile when notification is received that the vulnerability has been fixed.

20. The apparatus of claim 19, wherein the processor determines whether the vulnerability still exists and archives records associated with the vulnerability when the vulnerability does not still exist.

21. An apparatus for determining a criticality factor for a vulnerability in a computer system, comprising:

a memory for storing program instructions; and

a processor, configured according to the program instructions for entering in a database vulnerabilities identified during a vulnerability assessment, monitoring a frequency of occurrence for the identified vulnerabilities and assigning a vulnerability factor to a vulnerability based upon the frequency of occurrence of the vulnerability in the system.

22. The apparatus of claim 21, wherein the processor considers a criticality of an element in the system presenting the vulnerability and a rating of the severity of the vulnerability within the system when assigning a vulnerability factor.

23. An apparatus for providing automated tracking of security vulnerabilities, comprising:

means for storing program instructions; and

means configured according to the program instructions provided by the means for storing for performing a vulnerability assessment on a system, storing data obtained from the vulnerability assessment in a vulnerability database, determining a vulnerability score based on a plurality of vulnerability factors identified by the vulnerability assessment and determining a time to fix a vulnerability identified by the vulnerability assessment of the system based on the determined vulnerability score.

24. An apparatus for determining a criticality factor for a vulnerability in a computer system, comprising:

means for storing program instructions; and

means configured according to the program instructions provided by the means for storing for entering in a database vulnerabilities identified during a vulnerability assessment, monitoring a frequency of occurrence for the identified vulnerabilities and assigning a vulnerability factor to a vulnerability based upon the frequency of occurrence of the vulnerability in the system.

25. A program storage device readable by a computer, the program storage device tangibly embodying one or more programs of instructions executable by the computer to perform a method for providing automated tracking of security vulnerabilities, the method comprising:

performing a vulnerability assessment on a system;

storing data obtained from the vulnerability assessment in a vulnerability database;

determining a vulnerability score based on a plurality of vulnerability factors identified by the vulnerability assessment; and

determining a time to fix a vulnerability identified by the vulnerability assessment of the system based on the determined vulnerability score.

26. A program storage device readable by a computer, the program storage device tangibly embodying one or more programs of instructions executable by the computer to perform a method for determining a criticality factor for a vulnerability in a computer system, the method comprising:

entering in a database vulnerabilities identified during a vulnerability assessment;

monitoring a frequency of occurrence for the identified vulnerabilities; and

assigning a vulnerability factor to a vulnerability based upon the frequency of occurrence of the vulnerability in the system.